#2

i1046 U.S. PTO
09/976447
10/12/01

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 ７月 ４日

出願番号
Application Number: 特願２００１－２０２９５４

出願人
Applicant(s): アライドテレシス株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ８月３１日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号 出証特２００１－３０７８２９９

【書類名】　特許願
【整理番号】　IP217001
【提出日】　平成13年 7月 4日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 9/32
H04L 12/28
G06F 13/00
【発明者】
【住所又は居所】　東京都品川区西五反田７－２１－１１　アライドテレシス株式会社内
【氏名】　佐藤　貴之
【特許出願人】
【識別番号】　396008347
【氏名又は名称】　アライドテレシス株式会社
【代理人】
【識別番号】　100099818
【弁理士】
【氏名又は名称】　安孫子　勉
【手数料の表示】
【予納台帳番号】　064699
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　インテリジェント中継機器における不正アクセス回避方法、インテリジェント中継機器用不正アクセス回避プログラム、インテリジェント中継機器用不正アクセス回避プログラムを記録した記録媒体、インテリジェント中継機器及びＬＡＮシステム

【特許請求の範囲】

【請求項１】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器における不正アクセス回避方法であって、

外部の機器からのアクセスが前記ＴＣＰ／ＩＰプロトコルの実行によって認証された場合、当該外部の機器から送信されたパケットに含まれる送信元ＩＰアドレスを抽出して記憶し、以後、外部の機器からのアクセスが生じた場合、当該アクセスを行った外部の機器の送信元ＩＰアドレスが前記記憶された送信元ＩＰアドレスと一致するか否かを判定し、一致すると判定された場合にのみ当該送信元ＩＰアドレスを有する外部の機器と前記インテリジェント中継機器間の以後の通信を可能とすることを特徴とするインテリジェント中継機器における不正アクセス回避方法。

【請求項２】　送信元ＩＰアドレスが一致しないと判定された場合、その一致しなと判定された送信元ＩＰアドレスを不正アクセスＩＰリストに登録することを特徴とする請求項１記載のインテリジェント中継機器における不正アクセス回避方法。

【請求項３】　送信元ＩＰアドレスが一致しないと判定された場合、その一致しなと判定された送信元ＩＰアドレスを、認証を受けた管理用コンピュータへ通知することを特徴とする請求項１又は請求項２記載のインテリジェント中継機器における不正アクセス回避方法。

【請求項４】　送信元ＩＰアドレスが一致すると判定された場合、当該送信元ＩＰアドレスが予め設定された有効期限内のものであるか否かを判定し、有効期限内のものであると判定された場合にのみ当該送信元ＩＰアドレスを有する外

部の機器とインテリジェント中継機器間の以後の通信を可能とすることを特徴とする請求項１記載のインテリジェント中継機器における不正アクセス回避方法。

【請求項５】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行される不正アクセス回避プログラムであって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第１のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるＴＣＰ／ＩＰプロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第２のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第３のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第４のステップと、

前記第４のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元ＩＰアドレスを前記インテリジェント中継機器に抽出せしめると共に、記憶せしめる第５のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第６のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元ＩＰアドレスが、前記記憶された送信元ＩＰアドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第７のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスと

が一致するか否かの判定において、一致すると判定された場合には、送信元ＩＰアドレスが記憶されている送信元ＩＰアドレスと一致すると判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とすると共に、前記第２のステップから前記インテリジェント中継機器へ実行せしめる第８のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致しないと判定された場合には、送信元ＩＰアドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第９のステップと、

を具備してなることを特徴とするインテリジェント中継機器用不正アクセス回避プログラム。

【請求項６】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行される不正アクセス回避プログラムであって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第１のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるＴＣＰ／ＩＰプロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第２のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第３のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第４のステップと、

前記第４のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元ＩＰアドレスを前記インテリ

ジェント中継機器に抽出せしめると共に、記憶せしめる第５のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第６のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元ＩＰアドレスが、前記記憶された送信元ＩＰアドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第７のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元ＩＰアドレスが所定の有効期限内のものであるか否かを前記インテリジェント中継機器に判定せしめる第８のステップと、

前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元ＩＰアドレスを有する外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とすると共に、前記第２のステップから前記インテリジェント中継機器へ実行せしめる第９のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元ＩＰアドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第１０のステップと、

を具備してなることを特徴とするインテリジェント中継機器用不正アクセス回避プログラム。

【請求項７】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行される不正アクセス回避プログラムであって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第１のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるＴＣＰ／ＩＰプロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第２のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第３のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第４のステップと、

前記第４のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元ＩＰアドレスを前記インテリジェント中継機器に抽出せしめると共に、記憶せしめる第５のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第６のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元ＩＰアドレスが、前記記憶された送信元ＩＰアドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第７のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元ＩＰアドレスが所定の有効期限内のものであるか否かを前記インテリジェント中継機器に判定せしめる第８のステップと、

前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元ＩＰアドレスを有する外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とす

ると共に、前記第２のステップから前記インテリジェント中継機器へ実行せしめる第９のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元ＩＰアドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とすると共に、当該応答不可とされた外部の機器の送信元ＩＰアドレスを、前記インテリジェント中継機器に記憶せしめる第１０のステップと、

を具備してなることを特徴とするインテリジェント中継機器用不正アクセス回避プログラム。

【請求項８】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行される不正アクセス回避プログラムであって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第１のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるＴＣＰ／ＩＰプロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第２のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第３のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第４のステップと、

前記第４のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記

外部の機器からのパケット中に含まれている送信元ＩＰアドレスを前記インテリジェント中継機器に抽出せしめると共に、記憶せしめる第５のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第６のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元ＩＰアドレスが、前記記憶された送信元ＩＰアドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第７のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元ＩＰアドレスが所定の有効期限内のものであるか否かを前記インテリジェント中継機器に判定せしめる第８のステップと、

前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元ＩＰアドレスを有する外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とすると共に、前記第２のステップから前記インテリジェント中継機器へ実行せしめる第９のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元ＩＰアドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とすると共に、当該応答不可とされた外部の機器の送信元ＩＰアドレスを、所定の管理用コンピュータへ通知せしめる第１０のステップと、

を具備してなることを特徴とするインテリジェント中継機器用不正アクセス回避プログラム。

【請求項９】　第１０のステップで応答不可とされた外部の機器の送信元ＩＰアドレスを、所定の管理用コンピュータへ通知せしめる第１１のステップを具

備してなることを特徴とする請求項７記載のインテリジェント中継機器用不正アクセス回避プログラム。

【請求項１０】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行させる不正アクセス回避プログラムを記録した記録媒体であって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第１のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるＴＣＰ／ＩＰプロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第２のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第３のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第４のステップと、

前記第４のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元ＩＰアドレスを前記インテリジェント中継機器に抽出せしめると共に、記憶せしめる第５のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第６のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元ＩＰアドレスが、前記記憶された送信元ＩＰアドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第７のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスと

が一致するか否かの判定において、一致すると判定された場合には、送信元ＩＰアドレスが記憶されている送信元ＩＰアドレスと一致すると判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とすると共に、前記第２のステップから前記インテリジェント中継機器へ実行せしめる第８のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致しないと判定された場合には、送信元ＩＰアドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第９のステップと、

を具備してなることを特徴とするコンピュータ読み取り可能な不正アクセス回避プログラムを記録した記録媒体。

【請求項１１】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行させる不正アクセス回避プログラムを記録した記録媒体であって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第１のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるＴＣＰ／ＩＰプロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第２のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第３のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第４のステップと、

前記第４のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元ＩＰアドレスを前記インテリ

ジェント中継機器に抽出せしめると共に、記憶せしめる第５のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第６のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元ＩＰアドレスが、前記記憶された送信元ＩＰアドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第７のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元ＩＰアドレスが所定の有効期限内のものであるか否かを前記インテリジェント中継機器に判定せしめる第８のステップと、

前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元ＩＰアドレスを有する外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とすると共に、前記第２のステップから前記インテリジェント中継機器へ実行せしめる第９のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元ＩＰアドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第１０のステップと、

を具備してなることを特徴とするコンピュータ読み取り可能な不正アクセス回避プログラムを記録した記録媒体。

【請求項１２】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行させる不正アクセス回避プログラムを記録した記録媒体であって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第１のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるＴＣＰ／ＩＰプロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第２のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第３のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第４のステップと、

前記第４のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元ＩＰアドレスを前記インテリジェント中継機器に抽出せしめると共に、記憶せしめる第５のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第６のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元ＩＰアドレスが、前記記憶された送信元ＩＰアドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第７のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元ＩＰアドレスが所定の有効期限内のものであるか否かを前記インテリジェント中継機器に判定せしめる第８のステップと、

前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元ＩＰアドレスを有する外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とす

ると共に、前記第２のステップから前記インテリジェント中継機器へ実行せしめる第９のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元ＩＰアドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とすると共に、当該応答不可とされた外部の機器の送信元ＩＰアドレスを、前記インテリジェント中継機器に記憶せしめる第１０のステップと、

を具備してなることを特徴とするコンピュータ読み取り可能な不正アクセス回避プログラムを記録した記録媒体。

【請求項１３】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器において実行させる不正アクセス回避プログラムを記録した記録媒体であって、

前記インテリジェント中継機器に対して外部から最初のアクセスが発生したか否かを前記インテリジェント中継機器に判定せしめる第１のステップと、

外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるＴＣＰ／ＩＰプロトコルに基づいた認証処理を前記インテリジェント中継機器に行わしめる第２のステップと、

前記認証処理の終了後、当該認証が成立したか否かを前記インテリジェント中継機器に判定せしめる第３のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とし、今回のアクセスが初回か否かを前記インテリジェント中継機器に判定せしめる第４のステップと、

前記第４のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記

外部の機器からのパケット中に含まれている送信元ＩＰアドレスを前記インテリジェント中継機器に抽出せしめると共に、記憶せしめる第５のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とする第６のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元ＩＰアドレスが、前記記憶された送信元ＩＰアドレスと一致するか否かを前記インテリジェント中継機器に判定せしめる第７のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元ＩＰアドレスが所定の有効期限内のものであるか否かを前記インテリジェント中継機器に判定せしめる第８のステップと、

前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元ＩＰアドレスを有する外部の機器に対する前記インテリジェント中継機器による以後の応答を可能とすると共に、前記第２のステップから前記インテリジェント中継機器へ実行せしめる第９のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元ＩＰアドレスが一致しないと判定された外部の機器に対する前記インテリジェント中継機器による以後の応答を不可とすると共に、当該応答不可とされた外部の機器の送信元ＩＰアドレスを、所定の管理用コンピュータへ通知せしめる第１０のステップと、

を具備してなることを特徴とするコンピュータ読み取り可能な不正アクセス回避プログラムを記録した記録媒体。

【請求項１４】　第１０のステップで応答不可とされた外部の機器の送信元ＩＰアドレスを、所定の管理用コンピュータへ通知せしめる第１１のステップを

具備してなることを特徴とする請求項１２記載のコンピュータ読み取り可能な不正アクセス回避プログラムを記録した記録媒体。

【請求項１５】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器であって、

当該インテリジェント中継機器は、ＬＡＮ基幹線とのインターフェイス機能を有するＬＡＮ基幹線インターフェイス部と、

接続された端末とのインターフェイス機能を有するポートインターフェイス部と、

プログラム及びデータの記憶を行う記憶部と、

前記ＬＡＮ基幹線インターフェイス部と、前記ポートインターフェイス部と、前記記憶部の動作を制御する中央制御部とを具備し、

前記中央制御部は、外部の機器からのアクセスが前記ＴＣＰ／ＩＰプロトコルの実行によって認証された場合、当該外部の機器から送信されたパケットに含まれる送信元ＩＰアドレスを抽出して前記記憶部に記憶せしめ、以後、外部の機器からのアクセスが生じた場合、当該アクセスを行った外部の機器の送信元ＩＰアドレスが前記記憶された送信元ＩＰアドレスと一致するか否かを判定し、一致すると判定された場合にのみ当該送信元ＩＰアドレスを有する外部の機器との以後の通信が可能となるよう構成されてなることを特徴とするインテリジェント中継機器。

【請求項１６】　中央制御部は、送信元ＩＰアドレスが一致しないと判定された場合、その一致しなと判定された送信元ＩＰアドレスを記憶部の不正アクセスＩＰリストに登録することを特徴とする請求項１５記載のインテリジェント中継機器。

【請求項１７】　中央制御部は、送信元ＩＰアドレスが一致しないと判定された場合、その一致しなと判定された送信元ＩＰアドレスを、認証を受けた管理用コンピュータへ通知することを特徴とする請求項１５又は請求項１６記載のインテリジェント中継機器。

【請求項１８】　中央制御部は、送信元ＩＰアドレスが一致すると判定され

た場合、当該送信元ＩＰアドレスが予め設定された有効期限内のものであるか否かを判定し、有効期限内のものであると判定された場合にのみ当該送信元ＩＰアドレスを有する外部の機器とインテリジェント中継機器間の以後の通信を可能とすることを特徴とする請求項１５記載のインテリジェント中継機器。

【請求項１９】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器であって、

当該インテリジェント中継機器は、ＬＡＮ基幹線とのインターフェイス機能を有するＬＡＮ基幹線インターフェイス部と、

接続された端末とのインターフェイス機能を有するポートインターフェイス部と、

プログラム及びデータの記憶を行う記憶部と、

前記ＬＡＮ基幹線インターフェイス部と、前記ポートインターフェイス部と、前記記憶部の動作を制御する中央制御部とを具備し、

前記中央制御部は、外部から最初のアクセスが発生したか否かを判定する第１のステップと、

前記第１のステップにおいて、外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるＴＣＰ／ＩＰプロトコルに基づいた認証処理を行う第２のステップと、

前記認証処理の終了後、当該認証が成立したか否かを判定する第３のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する以後の応答を可能とし、今回のアクセスが初回か否かを判定する第４のステップと、

前記第４のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元ＩＰアドレスを抽出すると共に、当該送信元ＩＰアドレスを前記記憶部に記憶せしめる第５のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、

前記外部の機器に対する以後の応答を不可とする第６のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元ＩＰアドレスが、前記記憶された送信元ＩＰアドレスと一致するか否かを判定する第７のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致すると判定された場合には、送信元ＩＰアドレスが記憶されている送信元ＩＰアドレスと一致すると判定された外部の機器に対する以後の応答を可能とすると共に、前記第２のステップからの実行へ移行する第８のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致しないと判定された場合には、送信元ＩＰアドレスが一致しないと判定された外部の機器に対する以後の応答を不可とする第９のステップとを実行するよう構成されてなることを特徴とするインテリジェント中継機器。

【請求項２０】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器であって、

当該インテリジェント中継機器は、ＬＡＮ基幹線とのインターフェイス機能を有するＬＡＮ基幹線インターフェイス部と、

接続された端末とのインターフェイス機能を有するポートインターフェイス部と、

プログラム及びデータの記憶を行う記憶部と、

前記ＬＡＮ基幹線インターフェイス部と、前記ポートインターフェイス部と、前記記憶部の動作を制御する中央制御部とを具備し、

前記中央制御部は、外部から最初のアクセスが発生したか否かを判定する第１のステップと、

前記第１のステップにおいて、外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるＴＣＰ／ＩＰプロトコルに基づい

た認証処理を行う第２のステップと、

前記認証処理の終了後、当該認証が成立したか否かを判定する第３のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する以後の応答を可能とし、今回のアクセスが初回か否かを判定する第４のステップと、

前記第４のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元ＩＰアドレスを抽出すると共に、当該送信元ＩＰアドレスを前記記憶部に記憶せしめる第５のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する以後の応答を不可とする第６のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元ＩＰアドレスが、前記記憶された送信元ＩＰアドレスと一致するか否かを判定する第７のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元ＩＰアドレスが所定の有効期限内のものであるか否かを判定する第８のステップと、

前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元ＩＰアドレスを有する外部の機器に対する以後の応答を可能とすると共に、前記第２のステップからの実行へ移行する第９のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元ＩＰアドレスが一致しないと判定された外部の機器に対する以後の応答を不可とする第１０のス

テップとを実行するよう構成されてなることを特徴とするインテリジェント中継機器。

【請求項２１】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器であって、

当該インテリジェント中継機器は、ＬＡＮ基幹線とのインターフェイス機能を有するＬＡＮ基幹線インターフェイス部と、

接続された端末とのインターフェイス機能を有するポートインターフェイス部と、

プログラム及びデータの記憶を行う記憶部と、

前記ＬＡＮ基幹線インターフェイス部と、前記ポートインターフェイス部と、前記記憶部の動作を制御する中央制御部とを具備し、

前記中央制御部は、外部から最初のアクセスが発生したか否かを判定する第１のステップと、

前記第１のステップにおいて、外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるＴＣＰ／ＩＰプロトコルに基づいた認証処理を行う第２のステップと、

前記認証処理の終了後、当該認証が成立したか否かを判定する第３のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する以後の応答を可能とし、今回のアクセスが初回か否かを判定する第４のステップと、

前記第４のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元ＩＰアドレスを抽出すると共に、当該送信元ＩＰアドレスを前記記憶部に記憶せしめる第５のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する以後の応答を不可とする第６のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではない

と判定された場合に、当該アクセスのあった外部の機器の送信元ＩＰアドレスが、前記記憶された送信元ＩＰアドレスと一致するか否かを判定する第７のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元ＩＰアドレスが所定の有効期限内のものであるか否かを判定する第８のステップと、

前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元ＩＰアドレスを有する外部の機器に対する以後の応答を可能とすると共に、前記第２のステップからの実行へ移行する第９のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元ＩＰアドレスが一致しないと判定された外部の機器に対する以後の応答を不可とすると共に、当該応答不可とされた外部の機器の送信元ＩＰアドレスを、前記記憶部に記憶せしめる第１０のステップとを実行するよう構成されてなることを特徴とするインテリジェント中継機器。

【請求項２２】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器であって、

当該インテリジェント中継機器は、ＬＡＮ基幹線とのインターフェイス機能を有するＬＡＮ基幹線インターフェイス部と、

接続された端末とのインターフェイス機能を有するポートインターフェイス部と、

プログラム及びデータの記憶を行う記憶部と、

前記ＬＡＮ基幹線インターフェイス部と、前記ポートインターフェイス部と、前記記憶部の動作を制御する中央制御部とを具備し、

前記中央制御部は、外部から最初のアクセスが発生したか否かを判定する第１のステップと、

前記第１のステップにおいて、外部からの最初のアクセスが発生したと判定された場合に、ユーザ識別子とパスワードによるＴＣＰ／ＩＰプロトコルに基づいた認証処理を行う第２のステップと、

前記認証処理の終了後、当該認証が成立したか否かを判定する第３のステップと、

前記認証が成立したか否かの判定において、認証成立と判定された場合に、当該認証成立とされた外部の機器に対する以後の応答を可能とし、今回のアクセスが初回か否かを判定する第４のステップと、

前記第４のステップにおける外部機器の今回のアクセスが初回か否かの判定において、初回であると判定された場合に、前記認証処理において受信された前記外部の機器からのパケット中に含まれている送信元ＩＰアドレスを抽出すると共に、当該送信元ＩＰアドレスを前記記憶部に記憶せしめる第５のステップと、

前記認証が成立したか否かの判定において、認証不成立と判定された場合に、前記外部の機器に対する以後の応答を不可とする第６のステップと、

前記外部から最初のアクセスが発生したか否かの判定において、初回ではないと判定された場合に、当該アクセスのあった外部の機器の送信元ＩＰアドレスが、前記記憶された送信元ＩＰアドレスと一致するか否かを判定する第７のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスとが一致するか否かの判定において、一致すると判定された場合に、当該送信元ＩＰアドレスが所定の有効期限内のものであるか否かを判定する第８のステップと、

前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものであると判定された場合、当該送信元ＩＰアドレスを有する外部の機器に対する以後の応答を可能とすると共に、前記第２のステップからの実行へ移行する第９のステップと、

前記外部の機器の送信元ＩＰアドレスと前記記憶された送信元ＩＰアドレスと

が一致するか否かの判定において、一致しないと判定されたか、又は、前記送信元ＩＰが所定の有効期限内のものであるか否かの判定において、所定の有効期限内のものではないと判定されたかのいずれかの場合、前記送信元ＩＰアドレスが一致しないと判定された外部の機器に対する以後の応答を不可とすると共に、当該応答不可とされた外部の機器の送信元ＩＰアドレスを、所定の管理用コンピュータへ通知する第１０のステップとを実行するよう構成されてなることを特徴とするインテリジェント中継機器。

【請求項２３】　第１０のステップで応答不可とされた外部の機器の送信元ＩＰアドレスを、所定の管理用コンピュータへ通知する第１１のステップを具備してなることを特徴とする請求項２１記載のインテリジェント中継機器。

【請求項２４】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、ＬＡＮ基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなるＬＡＮシステムであって、

前記インテリジェント中継機器は、請求項１５記載のインテリジェント中継機器であることを特徴とするＬＡＮシステム。

【請求項２５】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、ＬＡＮ基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなるＬＡＮシステムであって、

前記インテリジェント中継機器は、請求項１６記載のインテリジェント中継機器であることを特徴とするＬＡＮシステム。

【請求項２６】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、ＬＡＮ基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなるＬＡＮシステムであって、

前記インテリジェント中継機器は、請求項１７記載のインテリジェント中継機器であることを特徴とするＬＡＮシステム。

【請求項２７】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、ＬＡＮ基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなるＬＡＮシステムであって、

前記インテリジェント中継機器は、請求項１８記載のインテリジェント中継機器であることを特徴とするＬＡＮシステム。

【請求項２８】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、ＬＡＮ基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなるＬＡＮシステムであって、

前記インテリジェント中継機器は、請求項１９記載のインテリジェント中継機器であることを特徴とするＬＡＮシステム。

【請求項２９】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、ＬＡＮ基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなるＬＡＮシステムであって、

前記インテリジェント中継機器は、請求項２０記載のインテリジェント中継機器であることを特徴とするＬＡＮシステム。

【請求項３０】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、ＬＡＮ基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなるＬＡＮシステムであって、

前記インテリジェント中継機器は、請求項２１記載のインテリジェント中継機

器であることを特徴とするＬＡＮシステム。

【請求項３１】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、ＬＡＮ基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなるＬＡＮシステムであって、

前記インテリジェント中継機器は、請求項２２記載のインテリジェント中継機器であることを特徴とするＬＡＮシステム。

【請求項３２】　複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器が、ＬＡＮ基幹線に接続される一方、前記インテリジェント中継機器には、前記複数のコンピュータが接続されてなるＬＡＮシステムであって、

前記インテリジェント中継機器は、請求項２３記載のインテリジェント中継機器であることを特徴とするＬＡＮシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、いわゆるＬＡＮ(Local Area Network)システムにおいて、パケットの中継機能などを有してなる中継機器に係り、特に、外部からの動作管理などが可能に構成されてなるわゆるインテリジェント中継機器におけるセキュリティの向上等を図ったものに関する。

【０００２】

【従来の技術】

いわゆるハブやルータなどに代表されるいわゆるパケット中継機器は、ＬＡＮシステムを構築する上で欠かせない機器であり、ＬＡＮシステムの形態等に応じて、基本的な機能に加えて様々な機能を有するものが種々提案されている（例えば、特開平５－３２７７２０号公報等参照）。このような中継機器において、特に、外部のコンピュータとの通信によって、その動作状況の把握や、動作条件の

設定などのいわゆる管理機能を有するものがあり、このような中継機器は、一般にインテリジェント中継機器と称されている。

従来、このようなインテリジェント中継機器を用いて構築されたＬＡＮシステムにおいて、このインテリジェント中継機器の各種の動作条件等を、ＬＡＮシステムに接続された管理用コンピュータからの遠隔操作により設定、変更する等の管理を可能とするために、インテリジェント中継機器にはＩＰアドレスが付与されており、管理用コンピュータとインテリジェント中継機器間の通信処理には、いわゆるＴＣＰ／ＩＰ通信処理が行われるようになっている。すなわち、具体的には、TELNET(RFC854)、SNMP(RFC1157)、TFTP(RFC1350)、ICMP(RFC792)、HTTP(RFC1945)などのいわゆるＴＣＰ／ＩＰプロトコルが管理用コンピュータとインテリジェント中継機器間の通信の形態に応じて種々選択的に用いられるようになっている。

例えば、インテリジェント中継機器を、管理者以外の不正操作から防ぐために従来は、TELNET(RFC854)によって当該インテリジェント中継機器へログインできるようにし、ログイン後にユーザ識別子とパスワードを入力せしめ、それが所定のものと一致する場合にのみ管理者からのアクセスとして認証し、外部からのそれ以後の操作が許可されるようなものとなっていた。

【０００３】

【発明が解決しようとする課題】

しかしながら、このような従来の構成にあって、そのセキュリティはもっぱらプロトコルに依存するものであり、ＴＣＰ／ＩＰプロトコルの中には、セキュリティ機能を有しないものもあり、決して信頼性の高いセキュリィティを保証するものではなかった。すなわち、上記従来装置の例で言えば、ログイン後のユーザ識別子とパスワードの入力による認証は、TELNETがその機能の一つとして有するものであり、インテリジェント中継機器への不正なアクセスを防止する観点から独自に付加された機能ではなく、しかも、ユーザ識別子とパスワードさえ一致していれば、管理用コンピュータ以外からのコンピュータからのアクセスであっても、容易に認証されてしまうという欠点があり、セキュリティの点で充分満足できるものではなかった。

【０００４】

本発明は、上記実状に鑑みてなされたもので、プロトコルのセキュリティ機能に依存することなく、しかも、予め指定されたコンピュータ以外からのアクセスを確実に断つことができるインテリジェント中継機器における不正アクセス回避方法、インテリジェント中継機器用不正アクセス回避プログラム、インテリジェント中継機器用不正アクセス回避プログラムを記録した記録媒体、インテリジェント中継機器及びＬＡＮシステムを提供するものである。

本発明の他の目的は、既存のソフトウェアに新たな機能を若干付加するだけで、セキュリティ機能の強化、ひいては信頼性の向上を図ることができるインテリジェント中継機器における不正アクセス回避方法、インテリジェント中継機器用不正アクセス回避プログラム、インテリジェント中継機器用不正アクセス回避プログラムを記録した記録媒体、インテリジェント中継機器及びＬＡＮシステムを提供することにある。

本発明の他の目的は、セキュリティに関するソフトウェアの簡素化を図ることができるインテリジェント中継機器における不正アクセス回避方法、インテリジェント中継機器用不正アクセス回避プログラム、インテリジェント中継機器用不正アクセス回避プログラムを記録した記録媒体、インテリジェント中継機器及びＬＡＮシステムを提供することにある。

【０００５】

【課題を解決するための手段】

上記発明の目的を達成するため、本発明に係るインテリジェント中継機器における不正アクセス回避方法は、

複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器における不正アクセス回避方法であって、

外部の機器からのアクセスが前記ＴＣＰ／ＩＰプロトコルの実行によって認証された場合、当該外部の機器から送信されたパケットに含まれる送信元ＩＰアドレスを抽出して記憶し、以後、外部の機器からのアクセスが生じた場合、当該アクセスを行った外部の機器の送信元ＩＰアドレスが前記記憶された送信元ＩＰア

ドレスと一致するか否かを判定し、一致すると判定された場合にのみ当該送信元ＩＰアドレスを有する外部の機器と前記インテリジェント中継機器間の以後の通信を可能とするよう構成されてなるものである。

【０００６】

かかる方法においては、一旦、ＴＣＰ／ＩＰプロトコルによる認証が成立した後は、そのプロトコルの実行際に外部の機器から送信されたパケットに包含されている送信元ＩＰアドレスを抽出して記憶しておくことで、それ以後、外部の機器からアクセスが生じた際に、この送信元ＩＰアドレスが一致しない場合には、応答不可とされるため、ユーザ識別子とパスワードが一致していれば、送信元ＩＰアドレスが異なる場合であってもアクセスが可能となってしまうという従来の不都合が確実に回避でき、従来に比して、簡易な構成でより一層のセキュリティの向上が図られることとなるものである。

【０００７】

また、本発明の目的を達成するため、本発明に係るインテリジェント中継機器は、

複数のコンピュータ間において授受されるパケットを中継する機能を有すると共に、外部の機器からＴＣＰ／ＩＰプロトコルに基づいて管理可能に構成されてなるインテリジェント中継機器であって、

当該インテリジェント中継機器は、ＬＡＮ基幹線とのインターフェイス機能を有するＬＡＮ基幹線インターフェイス部と、

接続された端末とのインターフェイス機能を有するポートインターフェイス部と、

プログラム及びデータの記憶を行う記憶部と、

前記ＬＡＮ基幹線インターフェイス部と、前記ポートインターフェイス部と、前記記憶部の動作を制御する中央制御部とを具備し、

前記中央制御部は、外部の機器からのアクセスが前記ＴＣＰ／ＩＰプロトコルの実行によって認証された場合、当該外部の機器から送信されたパケットに含まれる送信元ＩＰアドレスを抽出して前記記憶部に記憶せしめ、以後、外部の機器からのアクセスが生じた場合、当該アクセスを行った外部の機器の送信元ＩＰア

ドレスが前記記憶された送信元ＩＰアドレスと一致するか否かを判定し、一致すると判定された場合にのみ当該送信元ＩＰアドレスを有する外部の機器との以後の通信が可能となるよう構成されてなるものである。

【０００８】

かかる構成は、特に、請求項１記載の発明に係るインテリジェント中継機器における不正アクセス回避方法を実行するに適したもので、例えば、いわゆるマイクロコンピュータ、又は、それと同等の機能を有する回路とソフトウェアによって実現し得るものである。

【０００９】

【発明の実施の形態】

以下、本発明の実施の形態について、図１乃至図４を参照しつつ説明する。

なお、以下に説明する部材、配置等は本発明を限定するものではなく、本発明の趣旨の範囲内で種々改変することができるものである。

最初に、本発明の実施の形態におけるインテリジェント中継機器を用いて構成されたＬＡＮシステムについて、図１を参照しつつ説明する。

このＬＡＮシステムにおいて、インテリジェント中継機器１には、複数の端末としてのいわゆるパーソナルコンピュータ２が接続される一方、ＬＡＮ基幹線３が接続されている。このＬＡＮ基幹線３には、少なくとも管理用コンピュータ４が接続されるが、さらに、他のネットワーク５が接続されてもよい。そして、管理用コンピュータ４は、ＬＡＮ基幹線３に直接接続される形態の他、他のネットワーク５を介して接続される形態であってもよい。

なお、管理用コンピュータ４は、サーバを兼ねるものであってもよく、また、サーバは管理用コンピュータ４とは、別個に設けるようにしてもよい。

また、インテリジェント中継機器１は、ＯＳＩ参照モデルにおけるネットワーク層を含めてこれより上位の層、換言すれば、ＴＣＰ／ＩＰ(Transmission Control Protocol/Internet Protocol)におけるインターネット層より上位の層におけるパケット処理に対応できるよう構成されてなるものであるとする。

【００１０】

図２には、このインテリジェント中継機器１の構成例が示されており、以下、

同図を参照しつつ、その構成等について説明する。

このインテリジェント中継機器１は、中央制御部６と、ＬＡＮ基幹線インターフェイス部（図２においては「Ｂ－Ｉ／Ｆ」と表記）７と、ポートインターフェイス部（図２においては「Ｐ－Ｉ／Ｆ」と表記）８と、記憶部９とを有し、これらが共通内部バス１０を介して相互に接続されたものとなっているもので、中央制御部６によって後述するような不正アクセス回避処理がなされることを除けば、従来装置と基本的に変わるところはないものである。

かかる構成において、中央制御部６は、このインテリジェント中継機器１全体の動作制御を行うもので、特に、本発明の実施の形態においては、後述する不正アクセス回避処理が実行されるようになっている。

ＬＡＮ基幹線インターフェイス部７は、ＬＡＮ基幹線３と、このインテリジェント中継機器１とのいわゆるインターフェイスを図るものであり、また、ポートインターフェイス部８は、端末としてのパーソナルコンピュータ２とこのインテリジェント中継機器１とのいわゆるインターフェイスを図るものである。

記憶部９は、中央制御部６によって実行される各種のプログラムが記憶されると共に、ＬＡＮ基幹線インターフェイス部７やポートインターフェイス部８を介して取り込まれたデータや、また、これらを介して外部へ送出されるデータなどが記憶されるものとなっている。この記憶部９は、電源が断とされても記憶内容が消去されない領域と、電源の断によって記憶内容が消去される領域とを有してなるものとなっており、データなどの用途等に応じて、それぞれの領域に選択的に記憶されるようになっている。なお、このような記憶部９は、公知・周知の記憶素子などによって実現され得るもので、その詳細な説明は省略するが、例えば、いわゆるＲＯＭやＲＡＭなどの半導体メモリの他、ハードディスク等を用いて構成するのが好適である。

【００１１】

なお、本発明の実施の形態における記憶部９には、ＴＣＰ／ＩＰプロトコルが、電源が断とされても記憶内容が消去されない領域に記憶されており、中央制御部６によって必要に応じて実行されるものとなっている。なお、ＴＣＰ／ＩＰプロトコルには、種々あるが、後述するような不正アクセス回避処理の実行に適す

るものであれば特定のものに限定される必要はなく、より具体的には、ユーザ識別子とパスワードによるいわゆる認証処理が行われるものであることが必要である。

また、この記憶部９には、このインテリジェント中継機器１に予め付与されたＩＰアドレス、ＴＣＰ／ＩＰプロトコルに基づく外部の機器からのアクセスに対する認証に必要なユーザ識別子（ＩＤ）とパスワードが、電源が断とされても記憶内容が消去されない領域に予め記憶されている。

【００１２】

次に、中央制御部６によって実行される不正アクセス回避処理の第１の例について図３を参照しつつ説明する。

まず、前提として、この不正アクセス回避処理は、中央制御部６において実行されるメインルーチン処理の中で、一つのサブルーチン処理として実行されるようになっているものである。

中央制御部６による処理が開始されると、最初に、インテリジェント中継機器１へ対して外部からアクセスが生じたか否かが判定され（図３のステップＳ１００参照）、外部からのアクセス発生と判定されると（ＹＥＳの場合）、次のステップＳ１０２の処理へ進むこととなる。一方、ステップＳ１００において、外部からのアクセスが無いと判定された場合（ＮＯの場合）には、一旦、このサブルーチン処理を終了し、図示されないメインルーチン処理へ戻り、メインルーチン処理の所定の処理を経た後、再び、このサブルーチン処理が開始されることとなる。

【００１３】

そして、ステップＳ１０２においては、この外部からのインテリジェント中継機器１へ対するアクセスが初回であるか否かが判定され、初回であると判定された場合（ＹＥＳの場合）には、次述するステップＳ１１０の処理へ進む一方、初回ではないと判定された場合（ＮＯの場合）には、後述するステップＳ１０４の処理へ進むこととなる。

ステップＳ１１０においては、外部からインテリジェント中継機器１へアクセスを行った外部機器（例えば、管理用コンピュータ４）へ対してユーザ識別子（

ＩＤ）とパスワードが要求され、それらの入力受付が行われることとなる。

次いで、入力されたユーザ識別子とパスワードに対する認証処理が行われることとなる（図３のステップＳ１１２参照）。

【００１４】

ここで、先のステップＳ１１０及びステップＳ１１２の処理は、公知・周知のＴＣＰ／ＩＰプロトコルの実行処理によってなされるものである。すなわち、本発明の実施の形態におけるインテリジェント中継機器１は、先にその構成の説明において述べたように、ＴＣＰ／ＩＰプロトコルが搭載されたものを前提としており、特に、ユーザ識別子とパスワードによる認証処理が行われるものが好適である。このようなＴＣＰ／ＩＰプロトコルとしては、例えば、TELNETを挙げることができる。なお、このプロトコルの詳細な処理手順についてのここでの説明は省略することとする。

そして、認証処理（図３のステップＳ１１２参照）の終了後は、認証が成立したか否かが判定されることとなる（図３のステップＳ１１４参照）。ここで、認証の成立とは、ユーザ識別子及びパスワードが記憶部９に予め設定されているものと一致し、アクセスを行った外部機器へ対して認証が与えられる場合を言い、認証不成立とは、ユーザ識別子及びパスワードが記憶部９に予め設定されているものと一致せず、認証が与えられない場合を言う。

【００１５】

ステップＳ１１４において、認証成立せず、すなわち、認証不成立と判定された場合（ＮＯの場合）には、外部機器に対する応答不可とされて（図３のステップＳ１２２参照）、一連のサブルーチン処理を終了し、一旦、メインルーチン処理へ戻ることとなる。そして、メインルーチン処理においては、搭載されているＴＣＰ／ＩＰプロトコルに応じて、応答不可に対応する処理がなされることとなる。

一方、ステップＳ１１４において、認証成立と判定された場合（ＹＥＳの場合）には、外部機器からのアクセスに対する応答可とされて（図３のステップＳ１１６参照）、次いで、今回の処理が外部機器からの初回のアクセスに対応するものであるか否かが判定されることとなる（図３のステップＳ１１８参照）。そし

て、外部機器のアクセスが初回であると判定された場合（ＹＥＳの場合）には、次述するステップＳ１２０の処理へ進む一方、外部機器のアクセスが初回ではないと判定された場合（ＮＯの場合）には、既に、次述するステップＳ１２０の処理が行われており、再度の処理の必要がないため、一連のサブルーチン処理が終了されることとなり、メインルーチン処理へ戻ることとなる。

ステップＳ１２０の処理においては、外部機器から送信されたパケットに含まれる送信元（外部機器）のＩＰアドレス（以後「送信元ＩＰアドレス」と言う）が抽出され、記憶部９の所定の領域に記憶されることとなる（図３のステップＳ１１８参照）。なお、この場合、送信元ＩＰアドレスの記憶領域は、電源が断とされても記憶内容が消去されない領域が好適である。

このステップＳ１２０の処理が終了した後は、この一連のサブルーチン処理が終了されることとなり、メインルーチン処理へ戻ることとなる。そして、メインルーチン処理においては、搭載されているＴＣＰ／ＩＰプロトコルに応じて、応答可に対応する処理がなされることとなる。

【００１６】

また、先のステップＳ１０２において、初回のアクセスではないと判定されてステップＳ１０４へ進んだ場合には、アクセスを行ってきた外部機器（例えば、管理用コンピュータ４）の送信元ＩＰアドレスが、既に記憶部９に記憶されている送信元ＩＰアドレスと一致するか否かが判定されることとなる。なお、外部機器の送信元ＩＰアドレスは、当該外部機器からインテリジェント中継機器１へ送信されたパケット内に公知・周知の形式で含まれているものを抽出することで認識可能なものである。

そして、このステップＳ１０４において、送信元ＩＰアドレスが一致すると判定された場合（ＹＥＳの場合）には、アクセスの有った外部機器に対して応答可とされて、先のステップＳ１１０の処理へ進むこととなる（図３のステップＳ１０６参照）。一方、ステップＳ１０４において、送信元ＩＰアドレスが一致しないと判定された場合（ＮＯの場合）には、外部機器に対する応答不可とされて、一連のサブルーチン処理を終了し、メインルーチン処理へ戻ることとなる（図３のステップＳ１０８参照）。なお、メインルーチン処理においては、搭載されて

いるＴＣＰ／ＩＰプロトコルに応じて、応答不可に対応する処理がなされることとなる。

【００１７】

次に、中央制御部６によって実行される不正アクセス回避処理の第２の例について図４を参照しつつ説明する。なお、図３に示された処理と同一の内容の処理については、同一の符号を付してその詳細な説明を省略し、以下、異なる点を中心に説明することとする。

まず、この第２の例における不正アクセス回避処理の内容を概括的に述べれば、先の図３に示された第１の例における不正アクセス回避処理を基本として、アクセスを認める外部機器の送信元ＩＰアドレスに有効期間を設ける一方、送信元ＩＰアドレスが一致しない場合には、不正アクセスＩＰリストへ記憶すると共に、管理装置へ通知するようにしたものである。

以下、図４を参照しつつ、具体的に説明する。この図４に示されたサブルーチン処理において、図３に示されたサブルーチン処理と異なるのは、ステップＳ１０６，Ｓ１０９ａ，Ｓ１０９ｂが設けられた点にあり、他の処理内容は図３に示されたサブルーチン処理におけるものと同一であるので、以下、これらの異なる各々のステップの処理内容について説明することとする。

【００１８】

まず、ステップＳ１０４において、アクセスを行ってきた外部機器（例えば、管理用コンピュータ４）の送信元ＩＰアドレスが、既に記憶部９に記憶されている送信元ＩＰアドレスと一致すると判定された場合（ＹＥＳの場合）、この送信元ＩＰアドレスが有効期限内のものか否かが判定されることとなる（図４のステップＳ１０５参照）。すなわち、このインテリジェント中継機器１に対するアクセスを許容する外部機器の送信元ＩＰアドレスは、既に述べたように記憶部９の所定の領域に予め記憶されるが、その最初の記憶の際に有効期間を定め、ステップＳ１０５においては、その有効期限内であるか否かが判定されるようになっている。なお、有効期限を判定するためには、送信元ＬＩＰアドレスの記憶の時点からの時間の経過を認識する必要があるが、これは、公知・周知のソフトウェア処理によるいわゆるカレンダ機能、または、時計機能が中央制御部６において実

行されるようにすることで実現可能なものである。

そして、ステップＳ１０５において、有効期限内であると判定された場合（ＹＥＳの場合）には、アクセスの有った外部機器に対して応答可とされて、ステップＳ１１０の処理へ進むこととなる（図４のステップＳ１０６参照）。

【００１９】

一方、ステップＳ０４において、送信元ＩＰアドレスが一致しないと判定されたか又は、ステップＳ１０５において、有効期限内ではない、すなわち、換言すれば、有効期限切れであると判定されたか、いずれかの場合には、外部機器に対する応答不可とされて（図４のステップＳ１０８参照）、次いで、不正アクセスＩＰリストへ、ステップＳ１０４の判定において一致しないとされた外部機器の送信元ＩＰアドレスが登録されることとなる（図４のステップＳ１０９ａ参照）。すなわち、このインテリジェント中継機器１へ外部からのアクセスがあり、そのアクセスしてきた外部機器の送信元ＩＰアドレスが、ステップＳ１０４の判定において不一致とされた場合に、当該不一致とされた送信元ＩＰアドレスを登録しておくための不正アクセスＩＰリストが記憶部９の所定の領域に設けられており、そこへ逐次記憶されるようになっている。

次いで、この不一致とされた送信元ＩＰアドレスを、管理用コンピュータ４へ知らしめるべく、この送信元ＩＰアドレスが所定のパケットとして、ＬＡＮ基幹線インターフェイス部７を介して管理用コンピュータ４へ送信されることとなる（図４のステップＳ１０９ｂ参照）。そして、このステップ１０９ｂの処理後は、メインルーチン処理へ戻り、搭載されているＴＣＰ／ＩＰプロトコルに応じて、応答不可に対応する処理がなされることとなる。

【００２０】

なお、上述の第２の例においては、不一致とされた送信元ＩＰアドレスの記憶（図４のステップＳ１０９ａ参照）と、その送信元ＩＰアドレスの管理用コンピュータ４への通知（図４のステップＳ１０９ｂ参照）とを行うようにしたが、いずれか一方を行うようにしてもよい。

また、上述した第１及び第２のいずれの例においても、インテリジェント中継機器１に記憶されるアクセス可能な外部機器の送信元ＩＰアドレスは、一つであ

ることを前提として説明をしたが、一つに限定される必要はなく、複数設定されても勿論よいものである。

【００２１】

また、インテリジェント中継機器１が、ＴＣＰ／ＩＰネットワークにおけるネットワーク管理プロトコルであるＳＮＭＰ(Simple Network Management Protocol)に対応できるよう構成されたものである場合、すなわち、インテリジェント中継機器１にＳＮＭＰエージェントが搭載される一方、例えば、管理用コンピュータ４にＳＮＭＰマネージャが搭載されると共に、他のコンピュータにも、ＳＮＭＰマネージャが搭載される場合などにおいては、インテリジェント中継機器１からイベント通知(Trap)を送信する際の送信先として、特定のコンピュータに限定したい場合、例えば、管理用コンピュータ４のみをTrapの送信先としたい場合、その送信元ＩＰアドレスをインテリジェント中継機器１に管理装置情報として記憶しておくことで、管理用コンピュータ４のみにTrapが送信されるようにして、情報の不用意な拡散を防止することができるものとなる。

さらに、例えば、先の図３及び図４におけるステップＳ１１０，Ｓ１１２の認証処理を、暗号化してよりセキュリティの向上を図ってもよい。

【００２２】

なお、上述の構成例においては、中央制御部６によって実行されるインテリジェント中継機器用不正アクセス回避プログラムは、プログラムの記録媒体としての記憶部９の一部を構成する不揮発性の半導体メモリに記憶されており、この半導体メモリから中央制御部６に読み込まれて実行されることを前提として説明をしたが、記録媒体としては、半導体メモリに限定される必要がないことは勿論である。

すなわち、記録媒体としては、この他、フレキシブルディスクやＣＤ－ＲＯＭ、また、ＤＶＤ、ＰＤ等の光学記録媒体、ＭＤ等の光磁気記録媒体、磁気記録媒体等を用いても良いものである。なお、記録媒体によっては、その記録媒体専用のデータの読み出し、書き込みを行う装置が必要となり、それらを含めて記憶部９を構成しても良いことは勿論である。

【００２３】

【発明の効果】

以上、述べたように、本発明によれば、管理用コンピュータの送信元ＩＰアドレスを、既存のＴＣＰ／ＩＰプロトコルの実行処理において受信されたパケットから抽出して記憶し、以後、その送信元ＩＰアドレス以外のＩＰアドレスを有する外部の機器との通信を禁止するようにしたので、従来のＴＣＰ／ＩＰプロトコルの認証処理と相俟って、従来に比してよりセキュリティの向上を図ることができ、信頼性の高いシステムを提供することができるという効果を奏するものである。

また、送信元ＩＰアドレスが一致した後にＴＣＰ／ＩＰプロトコルによる認証処理を行えばよいので、種々のＴＣＰ／ＩＰプロトコルを搭載するものにあっては、いずれか一つのプロトコルによって認証処理が実行されるようにしておくことで十分なセキュリティが保持でき、個々のプロトコルの認証処理を省略することができため、ソフトウェアの負担を軽減することができるという効果を奏するものである。

さらに、ブロードキャストによるアクセスに対する応答も制限するこができるので、被管理機器、すなわち、管理用コンピュータによる管理の対象とされたインテリジェント中継機器の存在を、外部からの侵入者にとって識別困難なものとすることができ、従来に比してよりセキュリティの向上が図られることとなる。

また、従来、プロトコル毎に用意していたユーザ識別子やパスワードを一本化することができ、ソフトウェアの簡素化を図ることができるとい効果を奏するものである。

【図面の簡単な説明】

【図１】

本発明の実施の形態におけるＬＡＮシステムの構成例を示す構成図である。

【図２】

図１に示されたＬＡＮシステムに用いられるインテリジェント中継機器の構成例を示す構成図である。

【図３】

図２に示されたインテリジェント中継機器によって実行される不正アクセス回

避処理の第１の例における処理手順を示すサブルーチンフローチャートである。

【図４】

図２に示されたインテリジェント中継機器によって実行される不正アクセス回避処理の第２の例における処理手順を示すサブルーチンフローチャートである。

【符号の説明】

１…インテリジェント中継機器

３…ＬＡＮ基幹線

４…管理用コンピュータ

６…中央制御部

５…他のネットワーク

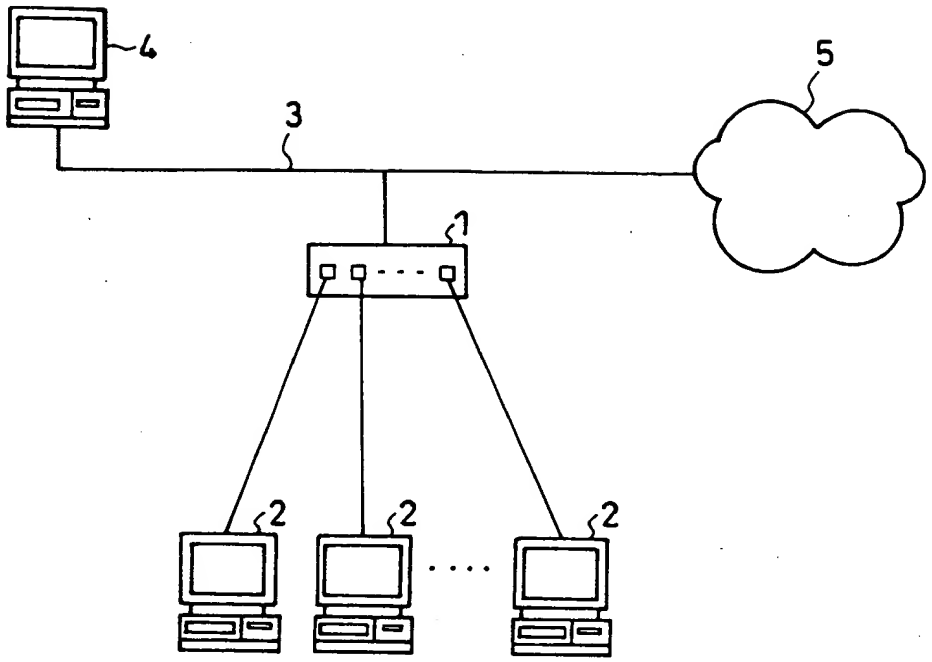
７…ＬＡＮ基幹線インターフェイス部

８…ポートインターフェイス部

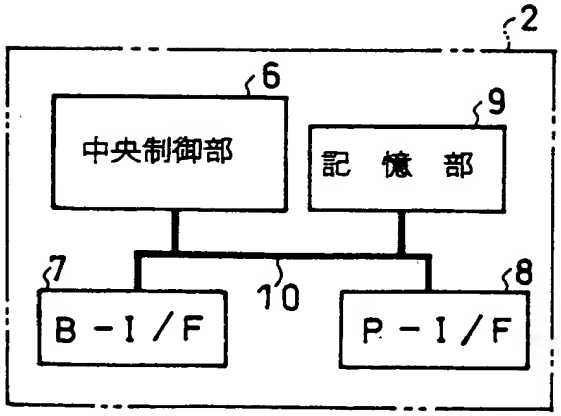
９…記憶部

【書類名】　　図面

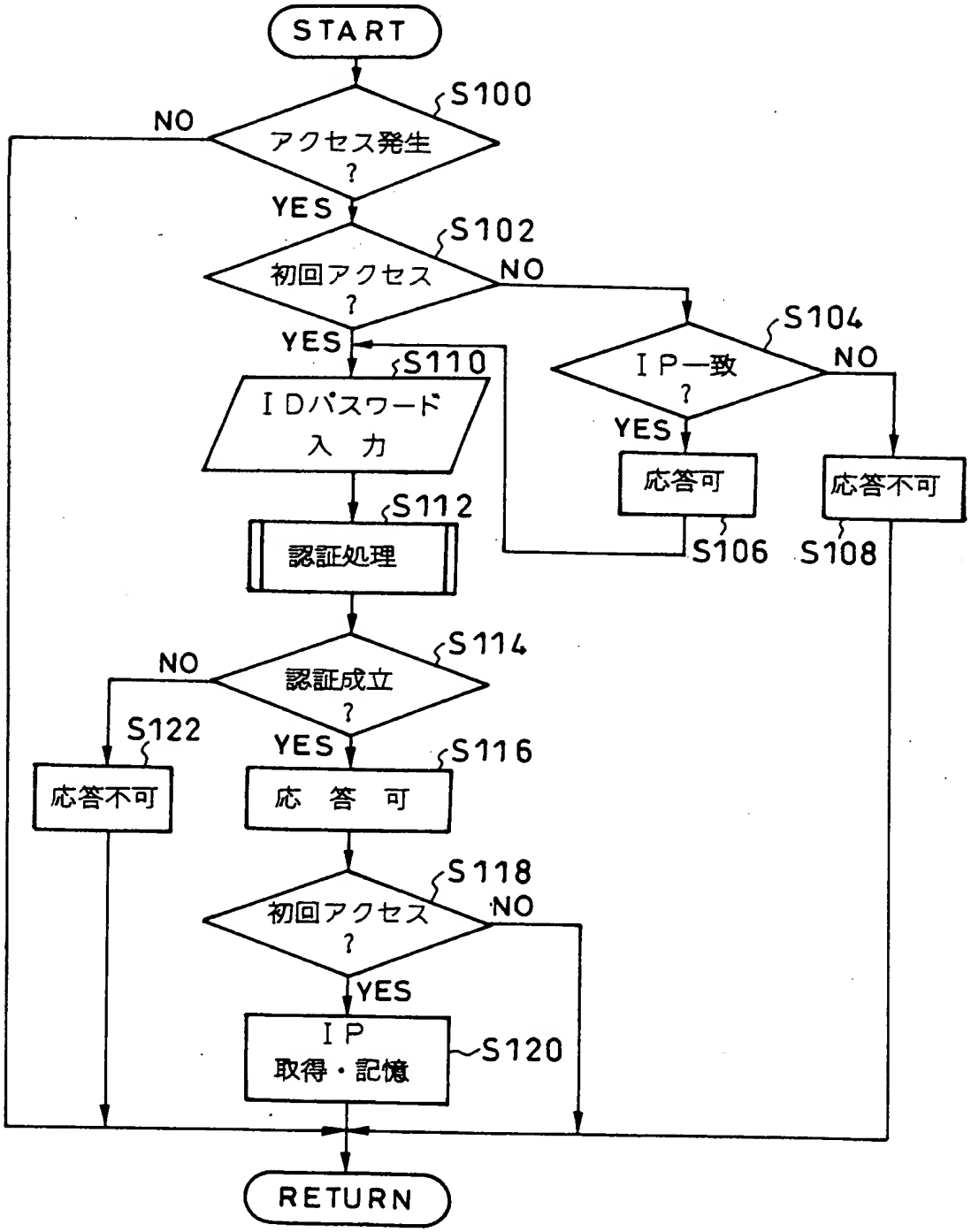
【図１】



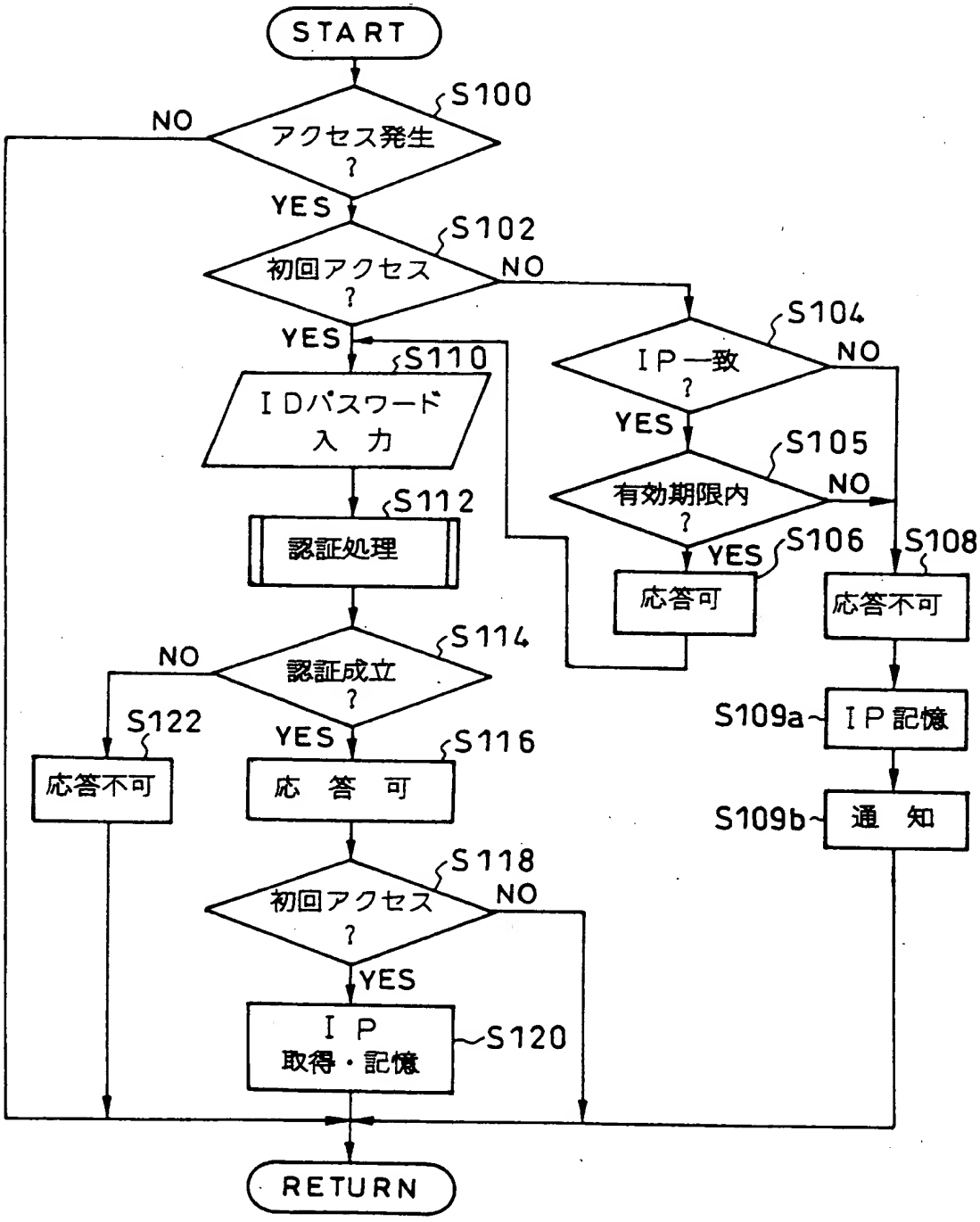
【図２】



【図３】


START
S100
アクセス発生
?
NO
YES
S102
初回アクセス
?
NO
YES
S104
IP一致
?
NO
YES
S110
IDパスワード
入力
S112
認証処理
応答可
S106
応答不可
S108
S114
認証成立
?
NO
YES
S122
応答不可
S116
応答可
S118
初回アクセス
?
NO
YES
IP
取得・記憶
S120
RETURN

【図４】


START
S100
アクセス発生
?
NO
YES
S102
初回アクセス
?
NO
YES
S104
IP一致
?
NO
YES
S105
有効期限内
?
NO
YES
S106
応答可
S108
応答不可
S109a
IP記憶
S109b
通知
S110
IDパスワード
入力
S112
認証処理
S114
認証成立
?
NO
YES
S116
応答可
S118
初回アクセス
?
NO
YES
S120
IP
取得・記憶
S122
応答不可
RETURN

【書類名】　　要約書

【要約】

【課題】　既存のソフトウェアに新たな機能を若干付加するだけで、セキュリティ機能の強化、信頼性の向上を図る。

【解決手段】　インテリジェント中継機器に対して外部の機器から最初にアクセスがあり、その外部の機器がインテリジェント中継機器におけるＴＣＰ／ＩＰプロトコルに基づく認証処理によって認証を得た場合、インテリジェント中継機器は、その外部の機器の送信元ＩＰアドレスを記憶し（ステップＳ１１４，Ｓ１１６，Ｓ１１８，Ｓ１２０）、以後、外部からアクセスが生じた場合、その送信元ＩＰアドレスが、先に記憶された送信元ＩＰアドレスと一致した場合にのみ、そのアクセスに対する応答を可能として（ステップＳ１０４，Ｓ１０６）、セキュリティの向上が図られている。

【選択図】　　図３

出　願　人　履　歴　情　報

識別番号　　〔３９６００８３４７〕

１．変更年月日　　２０００年１０月２４日
［変更理由］　住所変更
住　所　　東京都品川区西五反田７－２２－１７　ＴＯＣビル
氏　名　　アライドテレシス株式会社